

1-1-2016

The Right to Be Forgotten: Comparing U.S. and European Approaches

Samuel W. Royston
Ketterman, Rowland & Westlund, P.C.

Follow this and additional works at: <https://commons.stmarytx.edu/thestmaryslawjournal>



Part of the [Civil Rights and Discrimination Commons](#), [Comparative and Foreign Law Commons](#), [Constitutional Law Commons](#), [European Law Commons](#), [First Amendment Commons](#), [Law and Society Commons](#), [Legal Remedies Commons](#), and the [Privacy Law Commons](#)

Recommended Citation

Samuel W. Royston, *The Right to Be Forgotten: Comparing U.S. and European Approaches*, 48 ST. MARY'S L.J. 253 (2016).

Available at: <https://commons.stmarytx.edu/thestmaryslawjournal/vol48/iss2/4>

This Article is brought to you for free and open access by the St. Mary's Law Journals at Digital Commons at St. Mary's University. It has been accepted for inclusion in St. Mary's Law Journal by an authorized editor of Digital Commons at St. Mary's University. For more information, please contact sfowler@stmarytx.edu, jcrane3@stmarytx.edu.

ARTICLE

THE RIGHT TO BE FORGOTTEN: COMPARING U.S. AND EUROPEAN APPROACHES

SAMUEL W. ROYSTON*

Abstract	254
I. Introduction.....	254
II. The European Approach.....	255
A. <i>Google Spain SL v. Agencia Española de Protección de Datos</i> ..	256
B. Critical Reviews of <i>Google Spain SL v. AEPD</i>	260
C. The Max Mosley Cases	262
III. The U.S. Approach.....	264
A. Early American Right of Privacy Cases	265
1. <i>Melvin v. Reid</i>	265
2. <i>Sidis v. F-R Publishing Corp.</i>	267
B. The Restatement (Second) of Torts § 652.....	268
C. Instances of Internet Censorship Affecting United States Users.....	269
1. Google, Revenge Pornography, and De-linking Web Domains	269

* Samuel W. Royston is an Attorney at Tom Rhodes Law Firm, P.C. in San Antonio, Texas, where he joined in 2015 after obtaining his Juris Doctorate from St. Mary's University School of Law. He graciously thanks Professor Vincent R. Johnson and Meagan McKeown for their assistance and guidance in writing this paper and in navigating the balance among life, class, work, and the editorial board.

2. Erasure Button Laws.....	271
IV. Conclusion	273

ABSTRACT

This Article compares the European and United States stances regarding the right to be forgotten. Within that context, this Article explores the implications of technological advances on constitutional rights, specifically the intersection of the right to free speech and the right to privacy, commonly referred to as the “right to be forgotten” paradox. In the United States, the trend is to favor free speech, while Europe places an emphasis on human rights. Each approach is analyzed based on supporting case law. The consequences of each approach on society, both long- and short-term, are also discussed. This Article argues that a right to be forgotten is incompatible with American First Amendment jurisprudence and that online privacy and reputation management are best handled by the private sector as our culture continues to evolve with technology.

I. INTRODUCTION

Technology has infiltrated the everyday lives of most people living in the United States and Europe. The Internet in particular, has created a widespread ability to immediately access and transmit information on a global platform. This ability, while arguably the most beneficial technological advancement in human history, has carried with it several—perhaps unanticipated—societal consequences. The U.S. legal system and its fundamental principles have been challenged in many ways by the adoption of the Internet and modern technological advances.¹ The topic of this Article, the so-called “Right to Be Forgotten” Doctrine,² evidences

1. For example, the Communications Decency Act of 1996 addresses liability for defamatory statements posted on the web or transmitted via the Internet. 47 U.S.C. § 230 (2012). *See also* VINCENT R. JOHNSON, *ADVANCED TORT LAW: A PROBLEM APPROACH* 266-74 (2d ed. 2014) (discussing liability for defamation in the U.S. under the Communications Decency Act).

2. *See, e.g.*, Marcelo Thompson, *Beyond Gatekeeping: The Normative Responsibility of Internet Intermediaries*, 18 VAND. J. ENT. & TECH. L. 783, 809 (2016) (“[T]he Court of Justice of the European Union adopted what would become known, albeit hyperbolically, as the right to be forgotten. In *Google Spain SL*, the court recognized the right of individuals to have data about them removed from search engine results whenever such data is processed in incompatibility with provisions of the Data Protection Directive.”) (citation omitted). “The [Data Protection] Directive is due to be replaced by a directly effective E.U. Regulation. When this occurs, . . . [the Data Protection Act of 1998] will be repealed or significantly amended.” BRIAN NEILL ET AL., *DUNCAN AND NEILL ON DEFAMATION* 327 (4th ed. 2015).

one of these impediments, which courts have been increasingly forced to consider since the creation of the Internet. The controversy encompassing the right to be forgotten is found at the intersection between freedom of speech and the right to privacy. A person within a jurisdiction that has adopted the right to be forgotten is afforded an avenue to remove unwanted personal information from the Internet, often regardless of whether that person published the information in the first place. By doing so, that person's privacy rights are protected. Conversely, in a jurisdiction that does not recognize the right to be forgotten, a person has far less ability to remove truthful information published by another party; the other party's right to speak freely is protected. In other words, the right to be forgotten weighs the utility of allowing full access to uncensored information against the utility of protecting a person's image and well-being by allowing post-hoc censorship of information detrimental to that person.³ This balancing process is normally fact-intensive.⁴ On an international level, the balance between the rights to freedom of speech and privacy is unsettled with respect to the right to be forgotten. The right to be forgotten has garnered heated debate, with feverous supporting and opposing parties on each side. This debate has culminated into two opposing views between the United States and Europe, which have taken polar stances on whether to recognize a legal right to be forgotten. The U.S. approach tends to favor free speech over the right to privacy by refusing to recognize a constitutional right to be forgotten.⁵ On the other hand, European courts have expressly created a right to be forgotten, ruling in favor of content removal in certain contexts.

II. THE EUROPEAN APPROACH

The European approach to the right to be forgotten favors individual privacy at the expense of free expression, and the European Union (E.U.) expressly recognizes the doctrine as law.⁶ Through the doctrine, individuals

3. See *id.* at 338 (discussing balancing under the *Google Spain* decision).

4. See MULLIS ET AL., *GATLEY ON LIBEL AND SLANDER* 855–65 (12th ed. 2013) (explaining how the “ultimate balancing test” is applied in England).

5. The U.S. approach is consistent with the small number of American decisions that have refused to impose liability for invasion of privacy based on public disclosure of truthful information. See *Doe v. Methodist Hosp.*, 690 N.E.2d 681, 693 (Ind. 1997) (declining to recognize disclosure actions and noting that “torts involving disclosure of truthful but private facts . . . [encounter] a considerable obstacle in the truth-in-defense provisions of the Indiana Constitution.”); see also *Hall v. Post*, 372 S.E.2d 711, 717 (N.C. 1988) (declining to recognize tort liability for private disclosure of private facts because of its potential for conflict with the First Amendment to the Federal Constitution).

6. See Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)*, 2014 E.C.R. I-317, ¶¶ 54–55, <http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN> (affirming a right to be forgotten for citizens of the European Union).

in the E.U. are better able to control personal content on the Internet by making requests to search engines like Google that certain content be de-linked and no longer searchable.⁷ Search engines are required to accept de-linking requests from individuals, review them, and decide whether the request satisfies government-established guidelines.⁸ While those companies are often compelled to de-link information, they retain some discretion when determining what must be removed.⁹

A. Google Spain SL v. Agencia Española de Protección de Datos¹⁰

The landmark European case, which introduced the right to be forgotten into E.U. law, began after a Spanish man, Mario Costeja González, requested Google to remove personal information from its web search engine. Mr. Costeja González wanted Google to de-link online newspaper articles that reported his house was under foreclosure because he had missed two social security tax payments more than a decade earlier.¹¹ He filed a complaint with Spain's data-protection agency, the Agencia Española de Protección de Datos (AEPD), against the newspaper and Google, arguing that the online articles were outdated and irrelevant because the tax issues had been resolved years prior, and he was able to keep his home.¹² The AEPD dismissed the complaint against the newspaper, but the Google complaint proceeded.¹³ After upholding Mr. Costeja González's complaint

7. See *id.* at ¶¶ 98–99 (discussing how the data subject is entitled to have information linked to his name removed from Google and explaining “those rights override . . . the interest of the general public in having access to that information”).

8. See Farhad Manjoo, *Right to Be Forgotten' Online Could Spread*, N.Y. TIMES (Aug. 5, 2015), <http://nyti.ms/1SO0Bmk> (describing the process by which Europeans who feel they are being misrepresented by irrelevant or inaccurate search results can request search engines de-link the material).

9. See *Recent Case—Court of Justice of the European Union Creates Presumption that Google Must Remove Links to Personal Data upon Request—Case C-131/12*, Google Spain SL v. Agencia Española de Protección de Datos (May 13, 2014), 128 HARV. L. REV. 735, 737–38 (2014) (“[C]ritics argue these requests should not be considered or decided upon entirely inside a private corporation, without public accountability or scrutiny.”); Danny O'Brien & Jillian York, *Rights that Are Being Forgotten: Google, the ECJ, and Free Expression*, ELECTRONIC FRONTIER FOUND. (July 8, 2014), <https://www.eff.org/deeplinks/2014/07/rights-are-being-forgotten-google-ecj-and-free-expression> (discussing the risks inherent to companies like Google and Facebook becoming the frontline of content regulation and advocating that content restrictions should be determined by the courts rather than through an online form transmitted to a private company).

10. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), 2014 E.C.R. I-317, <http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN>.

11. *Id.* at ¶¶ 14–15.

12. *Id.* at ¶ 15.

13. See *id.* at ¶¶ 16–17 (“[T]he AEPD rejected the complaint in so far as it related to La

against Google and ordering Google to remove Mr. Costeja González's personal data from its search index, a request for preliminary rulings was submitted to the Court of Justice of the European Union (CJEU).¹⁴ The high court's request sought the CJEU's interpretation of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, (the Directive), as well as Article 8 of the Charter of Fundamental Rights of the European Union.¹⁵ Three questions were posed: (1) whether Directive 95/46 applies to companies operating outside the E.U.; (2) whether search engines are data "controllers" and thus subject to Directive 95/46; and (3) whether and under what circumstances citizens have the right to exercise the right to be forgotten.¹⁶

The CJEU first considered whether search engines such as Google are processors of personal data and must be regarded as data controllers within the meaning of Article 2 of Directive 95/46.¹⁷ Google Spain and Google, Inc. argued that search engines do not process data that appear on third parties' websites and which are displayed in a list of search results but rather "collect information available on the [I]nternet without effecting a selection between personal data and other information."¹⁸ Further, Google asserted that even if their search engines were to be considered "data processors," the company operating the search engine could not be said to be a "data controller" since the company had no knowledge of the data that appeared on extraneous websites, nor does the company operating the search engine

Vanguardia, taking the view that the publication by it of the information in question was legally justified as it took place upon order of the Ministry of Labour and Social Affairs and was intended to give maximum publicity to the auction in order to secure as many bidders as possible.").

14. *Id.* at ¶ 17.

15. *Id.* at ¶ 1. Directive 95/46 is aimed at protecting individuals' fundamental rights and freedoms, especially with regard to the right to privacy and the processing and free flow of personal data. *Id.* at ¶ 3; *see also* Council Directive 95/46, art. 2(a), 1995 O.J. (L 281) 31, 38 (EC) ("[D]ata-processing systems are designed to serve man . . . [and] they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy . . . and the well-being of individuals.").

16. *Google Spain SL*, Case C-131/12 at ¶ 20.

17. *Id.* at ¶¶ 21–41. Directive 95/46 defines "processing of personal data" or "processing" as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." Council Directive 95/46, art. 2(b), 1995 O.J. (L 281) 31, 38 (EC). The Directive defines "controller" as "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data". *Id.* art. 2(c).

18. *Google Spain SL*, Case C-131/12 at ¶ 22.

exercise any control over the data.¹⁹ The court found that:

[I]n exploring the [I]nternet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine “collects” such data which it subsequently “retrieves”, “records” and “organises” within the framework of its indexing programmes, “stores” on its servers and, as the case may be, “discloses” and “makes available” to its users in the form of lists of search results.²⁰

Thus, the court determined the Google search engines must be regarded as processing personal data within the meaning of Directive 95/46 Article 2(b).²¹ The court further reasoned that “the search engine operator . . . determines the purposes and means of” the processing of personal data and, therefore, must be considered a “controller” under the Directive.²²

The CJEU next considered whether the Directive applied to Google even though Google performed data processing outside of the country in which the complaint was filed.²³ The court held Google was subject to the Directive because Google, Inc. established a subsidiary, Google Spain, which promoted and sold advertising space in Spain and directed those activities towards inhabitants of Spain.²⁴

Finally, the CJEU reached the ultimate questions—whether Mr. González and other E.U. citizens may exercise a right to be forgotten, and

19. *Id.*

20. *Id.* at ¶ 28.

21. The court held the Google search engines are data processors within the meaning set forth in Directive 95/46, despite the fact that the search engine does not publish or alter the data and also collects, retrieves, and organizes other types of information without distinguishing such information from personal data. *Id.* at ¶¶ 28–29.

22. *Id.* at ¶ 33. The court equated search engine operators with controllers by discussing the role of the search engine in the greater distribution and accessibility of information that would not have otherwise been found on the web page where such information was published without a user searching for it through the search engine. *Id.* at ¶ 36.

23. *Id.* at ¶¶ 42–45. “Specifically, the main issues raised by the referring court concern the notion of ‘establishment’, within the meaning of Article 4(1)(a) of Directive 95/46, and of ‘use of equipment situated on the territory of the said Member State’, within the meaning of Article 4(1)(c).” *Id.* at ¶ 44.

24. *See id.* at ¶¶ 45–60 (observing how “Google Spain engages in the effective and real exercise of activity through stable arrangements in Spain” and is a separate legal entity from Google, Inc. on Spanish territory, thus making Google Spain an establishment of Google Inc. under Article 4(1)(a) of the Directive); *see also Court of Justice of the European Union Creates Presumption that Google Must Remove Links to Personal Data upon Request—Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos*, *supra* note 9, 737–38 (“Though all of Google Inc.’s data processing occurred outside Spain, Google Spain sold advertising space within the country; since advertising is Google Inc.’s main source of revenue, the court held that the two entities were ‘closely linked.’ Google Spain was thus effectively an establishment of Google Inc., making Google Inc. subject to the Directive.” (citing *Google Spain SL*, Case C-131/12 at ¶¶ 44, 60)).

consequently whether search engines like Google must remove personal information in accordance with requests from individuals.²⁵ The court discussed Article 12 of the Directive, which states: “Member States are to guarantee every data subject the right to obtain from the controller, as appropriate, the rectification, erasure or blocking of data the processing of which does not comply with the provisions of Directive 95/46, in particular because of the incomplete or inaccurate nature of the data.”²⁶ Then, the court discussed Article 7’s test for appropriateness of processing personal data:

[Article 7] permits the processing of personal data where it is necessary for the purposes of the legitimate interests pursued by the controller . . . except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject—in particular his right to privacy with respect to the processing of personal data—which require protection under . . . the [D]irective.²⁷

Finally, the court held that the Directive established the right to be forgotten.²⁸ According to the CJEU, when a data subject, such as Mr. González, takes issue with personal data, the data subject can make a request under Article 12(b) directly to the data controller (e.g., Google).²⁹ The data controller must then examine the request and, if meritorious, honor the request and end processing of the data in question. As for Mr. González’s requests to have his personal data removed by Google, the CJEU noted that the Directive called for a balancing test to determine whether the controller’s legitimate interests were “overridden by the interests or

25. *Google Spain SL*, Case C-131/12 at ¶ 62.

26. *Id.* at ¶ 70.

27. *Id.* at ¶ 74.

28. The phrase “the right to be forgotten” appears twice in the CJEU’s opinion—first in quoted language from the AEPD’s pleadings and second in paragraph 91, where it states that the fundamental rights to protect personal data and to privacy comprise the right to be forgotten. *Id.* at ¶¶ 20, 91 (“[T]he data subject may oppose the indexing by a search engine of personal data relating to him where their dissemination through the search engine is prejudicial to him and his fundamental rights to the protection of those data and to privacy—which encompass the ‘right to be forgotten’ . . .”). However, the phrase has become synonymous with an individual’s right to protect his or her personal data online.

29. *Id.* at ¶ 94 (“Therefore, if it is found, following a request by the data subject pursuant to Article 12(b) of Directive 95/46, that the inclusion in the list of results displayed following a search made on the basis of his name of the links to web pages published lawfully by third parties and containing true information relating to him personally is, at this point in time, incompatible with Article 6(1)(c) to (e) of the directive because that information appears, having regard to all the circumstances of the case, to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine, the information and links concerned in the list of results must be erased.”).

fundamental rights and freedoms of the data subject—in particular his right to privacy.”³⁰ Although the processing of some personal data is permitted when the controller’s legitimate interests require it, the controller’s economic interests are not enough to overcome the interference with the data subject’s privacy rights.³¹ In fact, the CJEU went as far as to state that “as a rule,” the data subject’s right to have information relating to him or her personally no longer linked to a list of search results based on his or her name overrides a search engine operator’s economic interest and “the interest of the general public in having access to that information upon a search relating to the data subject’s name.”³² Moreover, the court held it was not necessary that the information in question be proved prejudicial against the data subject before his or her rights to have it removed from search results would outweigh the search engine operator’s rights as a controller.³³ The CJEU concluded there was no public need for the information at issue in Mr. González’s case and no reason to deny Mr. González’s removal request.³⁴ The public utility for the information was outweighed by the detriment to the individual.³⁵ Several critics of the ruling, both American and European, have taken the stance that this precedent shifts too much power to the individual.³⁶

B. *Critical Reviews of Google Spain SL v. AEPD*

Critics from countries across the world have expressed numerous concerns regarding the CJEU’s holding in *Google Spain SL v. Agencia Española de Protección de Datos* and the right to be forgotten. At the outset, critics argue the evaluation criteria—“inadequate, irrelevant or no longer relevant, or excessive in relation to [the] purposes [of the processing] and in the light of the time that has elapsed”—gives far too much power to the individual and

30. *Id.* at ¶ 74; see also Charter of Fundamental Rights of the European Union, art. 8, 2000 O.J. (C 364) 1 (setting forth the right to protection of personal data).

31. *Google Spain SL*, Case C-131/12 at ¶ 81.

32. *Id.* at ¶ 99.

33. *Id.* at ¶ 99. But see *id.* (“However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question.”).

34. *Id.* at ¶ 98.

35. *Id.* at ¶ 98 (finding no substantial interest for the public in having Mr. González’s information).

36. See *Court of Justice of the European Union Creates Presumption that Google Must Remove Links to Personal Data upon Request—Case C-131/12*, *Google Spain SL v. Agencia Española de Protección de Datos*, *supra* note 9, 737–38 (discussing various criticisms of the case and citing multiple American and European sources).

offers insufficient credit to the basic fundamental rights of others, including freedom of expression and the right to information.³⁷ This unbalanced balancing test creates a presumption of erasure. Moreover, search engines, such as Google, become the gatekeepers to the proverbial erase button, removing links and data from the Internet at the request of individuals who prefer that information not be easily accessible. Google has already been forced to process hundreds of thousands of individual erasure requests,³⁸ and there is little incentive for them to thoroughly investigate those requests.³⁹ Instead, to avoid litigation or negative publicity relating to any request for removal, companies will likely honor most requests without conducting any meaningful investigations of the requests' merits.⁴⁰ Thus, while the Directive and the court's interpretation of the Directive go to great lengths to protect individuals' right to privacy, they fail to give any credence to freedom of expression and the free flow of information.⁴¹

Another line of criticism of the CJEU's opinion in the *Google Spain* case asserts that the court's interpretation of "data controllers" is overly broad and a proper interpretation of data controllers should not include search engine operators. A report by the British House of Lords analyzing the CJEU's decision stated that, by the court's logic, a search-engine user would be a data controller within the meaning of Directive 95/46;⁴² thus, every

37. *Id.* (quoting *Google Spain SL*, Case C-131/12 at ¶ 93); see also *id.* at 739–40 ("By focusing so much on the right to privacy, the CJEU 'forgot that other rights were also applicable,' including freedom of information." (footnote omitted) (citing Steve Peers, *The CJEU's Google Spain Judgment: Failing to Balance Privacy and Freedom of Expression*, E.U. L. ANALYSIS (May 13, 2014), <http://eulawanalysis.blogspot.co.uk/2014/05/the-cjeu-google-spain-judgment-failing.html>)).

38. See Sylvia Tippmann & Julie Powles, *Google Accidentally Reveals Data on 'Right to Be Forgotten' Requests*, GUARDIAN (July 14, 2015, 9:28), <https://www.theguardian.com/technology/2015/jul/14/google-accidentally-reveals-right-to-be-forgotten-requests> (stating the number of removal requests received by Google between May 2014 and July 2015 exceeded 280,000).

39. See Jeff John Roberts, *The Right to Be Forgotten from Google? Forget It, Says U.S. Crowd*, FORTUNE (Mar. 12, 2015, 11:32 AM), <http://fortune.com/2015/03/12/the-right-to-be-forgotten-from-google-forget-it-says-u-s-crowd> (discussing the decision search engines like Google will have to make between granting the request or "risking an expensive legal headache").

40. Cf. O'Brien & York, *supra* note 9 (discussing the risks inherent to companies like Google and Facebook becoming the frontline of content regulation).

41. See EU Court Enshrines "Right to Be Forgotten" in Spanish Case Against Google, REPORTERS WITHOUT BORDERS (May 14, 2014), <http://en.rsf.org/union-europeenne-eu-court-enshrines-right-to-be-14-05-2014,46278.html> (interpreting the ruling in *Google Spain* as holding privacy rights superior to the freedom of information).

42. See EUROPEAN UNION COMMITTEE, EU DATA PROTECTION LAW: A 'RIGHT TO BE FORGOTTEN?', 2014–2015, HL 40, ¶ 41 (U.K.) [hereinafter HL COMMITTEE REPORT] ("If search engines are data controllers, so logically are users of search engines."); see also O'Brien & York, *supra* note 9 ("Restrictions on free expression need to be considered, in public, by the courts, on a case-by-case basis, and with both publishers and plaintiffs represented, not via an online form . . .").

time an individual runs a Google search, they could become subject to the directive as a controller of the personal data of another.

Supporters of the court's opinion argue that critics have skewed the court's viewpoints and fail to see the opportunity the court provided to address the right to be forgotten with adequate regulatory standards. "Critics seeking meaningful change should instead use the decision and the ensuing debate to shape the conversation on a new regulatory regime tailored to the nuances of modern privacy protection and reflective of the values these critics seem to believe are currently underrepresented."⁴³

C. *The Max Mosley Cases*

Another case at the forefront of Europe's implementation of the right to be forgotten involves Max Mosley, former racecar driver and former President of the Fédération Internationale de l'Automobile (the governing body for Formula One racing).⁴⁴ An undercover journalist for news-outlet *News of the World* used a hidden camera to videotape Mr. Mosley allegedly engaging in a Nazi-themed group sex party with several women, supposedly prostitutes.⁴⁵ Mr. Mosley sued the newspaper for breach of confidence and the unauthorized disclosure of personal information after it published an article and photographs.⁴⁶ Mr. Mosley was awarded £60,000, but the court refused to grant an injunction ordering removal of the video, holding that because the video was so widely available, ordering the *News of the World* to remove it would serve no purpose.⁴⁷ Despite the court's holding in Mr.

43. *Court of Justice of the European Union Creates Presumption that Google Must Remove Links to Personal Data upon Request—Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (May 13, 2014)*, *supra* note 9 at 737–38; *see also id.* ("The real debate is not on what has already been decided, but on what is yet to come; if critics hope to change the substantive outcome, they must shift their focus from secondary legal and policy arguments to the fundamental values at stake.").

44. Ulrike Dauer & Lisa Fleisher, *Former Formula One Chief Max Mosley Settles Legal Dispute with Google: Harbinger of Battles to Come in Europe's Developing Right to Be Forgotten*, WALL ST. J. (May 15, 2015, 2:38 PM), <http://www.wsj.com/articles/former-formula-one-chief-max-mosley-settles-legal-dispute-with-google-1431702038>.

45. *See* Leigh Holmwood & Caitlin Fitzsimmons, *Max Mosley Wins £60,000 in Privacy Case*, GUARDIAN (July 24, 2008, 06:42), <http://www.theguardian.com/uk/2008/jul/24/mosley.privacy> (expressing the news outlet had an informant on Mosley's sex session).

46. *See* Mosley v. News Grp. Newspapers Ltd. [2008] EWHC (QB) 1777 [3] (Eng.) ("The cause of action is breach of confidence and/ or the unauthorized disclosure of personal information, said to infringe the Claimant's rights of privacy."); Holmwood & Fitzsimmons, *supra* note 45 (discussing Mosley's suit against the "paper for grossly invading his privacy after it printed pictures and published video of him indulging in a five-hour sadomasochistic sex session").

47. Mosley v. United Kingdom, App. No. 48009/08, Eur. Ct. H.R. para. 28 (2011); John Oates, *Max Mosley Loses Battle to Get Sex Video Off Web: NoTW Reposts 'Orgy' Footage*, REGISTER (Apr. 9, 2008, 14:12), http://www.theregister.co.uk/2008/04/09/formula_one_boss.

Mosley's case against the newspaper, Mr. Mosley continued to pursue injunctive relief by filing complaints against Google in Germany, France, and the United Kingdom.⁴⁸ Mr. Mosley prevailed at the trial court level in Germany and France, and the U.K. High Court of Justice permitted Mr. Mosley's case to proceed to trial; however, the parties reached a settlement agreement before the U.K. Court or the German and French appellate courts rendered opinions.⁴⁹ Some commentators have suggested that, had the various courts issued opinions, the right to be forgotten and the CJEU's ruling in the *Google Spain* case would not have applied to Mr. Mosley's case because of his status as a public figure.⁵⁰

Apart from Mr. Mosley's cases against Google, Mr. Mosley sought relief from the European Court of Human Rights (ECHR).⁵¹ Mr. Mosley argued that U.K. law should provide an opportunity for courts to issue pre-publication injunctions against news articles such as the article at issue in Mr. Mosley's case.⁵² The basis for his complaint was that the United Kingdom failed to protect his rights under Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms.⁵³ He reasoned that "it was for the courts and not the newspapers" to balance "the right to freedom of expression [with] the right to respect for private life."⁵⁴ While the ECHR criticized the newspaper's conduct, it refused to recognize a pre-notification requirement:

[T]he Court has consistently emphasised the need to look beyond the facts of the present case and to consider the broader impact of a pre-notification requirement. . . . [H]aving regard to the chilling effect to which a pre-notification requirement risks giving rise, to the significant doubts as to the effectiveness of any pre-notification requirement and to the wide margin of appreciation in this area, the Court is of the view that Article 8 does not

48. See Dauer & Fleisher, *supra* note 44 ("Mr. Mosley also won legal battles against Google in Paris and in Hamburg, Germany In January, the U.K. High Court of Justice allowed Mr. Mosley's claim to proceed to trial . . .").

49. *Id.*

50. See *id.* (explaining the balance that should occur between the right to privacy and the public's right to know).

51. Mosley v. United Kingdom, App. No. 48009/08, Eur. Ct. H.R. (2011).

52. *Id.* at ¶¶ 79–80.

53. See *id.* at ¶ 66 (2011) (quoting Art. 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms) ("1. Everyone has the right to respect for his private and family life 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.").

54. *Id.* at ¶ 80.

require a legally binding pre-notification requirement. Accordingly, the Court concludes that there has been no violation of Article 8 of the Convention by the absence of such a requirement in domestic law.⁵⁵

The ECHR also warned that instituting a pre-notification requirement before a newspaper or other media outlet publishes information about an individual would run the risk of violating Article 10—Freedom of Expression.⁵⁶

III. THE U.S. APPROACH

The doctrine of the right to be forgotten has been flatly rejected in U.S. courts, which favor free speech over privacy.⁵⁷ The United States' deference to the right to free speech is derived from the constitutional principles protecting the right to openly and freely obtain and transmit information.⁵⁸ In favoring free speech over privacy rights within the right-to-be-forgotten context, the American legal system does not altogether ignore the importance of protecting a person's privacy. American courts have almost uniformly adopted the approach taken in the Restatement (Second) of Torts which establishes a cause of action based on four distinct types of invasion of privacy.⁵⁹ However, U.S. courts have limited the tort causes of action surrounding privacy and prevented recovery where a person's past has been opened to the public.⁶⁰ While U.S. courts have, in

55. *Id.* at ¶¶ 130, 132. See also Mark Sweney, *Max Mosley Loses European Privacy Case*, GUARDIAN (May 10, 2011, 04:40), <http://www.theguardian.com/media/2011/may/10/max-mosley-loses-european-privacy-case> (discussing the ECHR's opinion and the chilling effect that a pre-notification system would have on the media).

56. *Mosley*, App. No. 48009/08 at ¶ 89.

57. See *Garcia v. Google, Inc.*, 786 F.3d 733, 745 (9th Cir. 2015) (en banc) ("Ultimately, Garcia would like to have her connection to the film forgotten and stripped from YouTube. Unfortunately for Garcia, such a 'right to be forgotten,' although recently affirmed by the Court of Justice for the European Union, is not recognized in the United States.").

58. See *id.* at 744–45 (citations omitted) (explaining the purpose for including copyright protections in the U.S. Constitution was to promote and stimulate the free exchange of ideas).

59. RESTATEMENT (SECOND) OF TORTS § 652A cmt. b (AM. LAW INST. 1977); see also Johnson, *supra* note 1, at 346 ("Claims arising from postings on social networking websites or from the contents of e-mail attachments are routinely scrutinized in terms of the language found in the second Restatement."). For present purposes, the most relevant privacy action is public disclosure of private facts. See RESTATEMENT (SECOND) OF TORTS § 652D (1977) ("One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.").

60. See *N.Y. Times Co. v. Sullivan*, 376 U.S. 254, 283 (1964) (creating the "actual malice" standard for defamation cases involving public officials); see also *Curtis Publ'g Co. v. Butts*, 388 U.S. 130, 164 (1967) (Warren, C.J., concurring) (expanding the "actual malice" standard to include public figures).

some situations, protected a person's private life after it has been published to the world, courts evenly reject the right to be forgotten in furtherance of protecting free speech. With some exceptions, rather than silencing speech, U.S. courts generally respect the principle that once a person or topic is public knowledge, it remains public knowledge.

A. *Early American Right of Privacy Cases*

1. *Melvin v. Reid*⁶¹

The first U.S. case indirectly focusing on the right to be forgotten was decided in *Melvin v. Reid* in 1931 by the California Fourth District Court of Appeals.⁶² A former prostitute, who was wrongfully accused of murder and acquitted at trial, adopted a more respectable lifestyle.⁶³ Having exchanged her life of ill-repute for a respectable life as a homemaker, the last thing she wanted was an open book into her past transgressions.⁶⁴ However, she subsequently became the subject of a movie entitled *The Red Kimono*, which was based on her trial.⁶⁵ It included the former prostitute's name and other facts pertaining to her former life—all of which were true facts contained within public court records.⁶⁶ In response, she filed suit, complaining the defendants violated her right to privacy.⁶⁷ The court first noted that it could find no California law creating a tort cause of action for violation of privacy; however, it rationalized that the California Constitution's guarantees of life, liberty, and the pursuit of happiness potentially established a cause of action for a violation of privacy.⁶⁸ In holding that the plaintiff had properly alleged a cause of action arising from the violation of privacy rights, the court explained that "the right of privacy may be defined as the right to live one's life in seclusion, without being subjected to unwarranted and undesired

"Public figure" means those persons who are "intimately involved in the resolution of important public questions or, by reason of their fame, shape events in areas of concern to society at large." *Id.*

61. *Melvin v. Reid*, 297 P. 91 (Cal. Dist. Ct. App. 1931).

62. See generally William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 392 (1960) (describing *Melvin* as "the leading case").

63. *Melvin*, 297 P. at 91.

64. See *id.* at 93 (explaining Melvin's life "should have been permitted to continue its course without having her reputation and social standing destroyed by the publication").

65. *Id.* at 91.

66. *Id.* at 91, 93. But see *Cox Broad. Corp. v. Cohn*, 420 U.S. 469, 496 (1975) (holding the First Amendment prohibits invasion of privacy claims when the information publicly disclosed is public record).

67. *Melvin*, 297 P. at 91 (Cal. Dist. Ct. App. 1931).

68. *Id.* at 93.

publicity. . . . the right to be let alone.”⁶⁹ The court qualified this definition, stating: “There are times, however, when one, whether willingly or not, becomes an actor in an occurrence of public or general interest. . . . [and] emerges from his seclusion, and it is not an invasion of his right of privacy to publish his photograph with an account of such occurrence.”⁷⁰ Although the court held that the plaintiff’s violation-of-privacy claim was actionable, it alluded to the fact that public information generally must remain public:

[T]he use of the incidents from the life of appellant in the moving picture is in itself not actionable. These incidents appeared in the records of her trial for murder, which is a public record, open to the perusal of all. The very fact that they were contained in a public record is sufficient to negative the idea that their publication was a violation of a right of privacy. When the incidents of a life are so public as to be spread upon a public record, they come within the knowledge and into the possession of the public and cease to be private.⁷¹

The court’s recognition of Plaintiff’s claim was grounded in a desire to protect her identity and former life, which were vital to providing her with the means of obtaining rehabilitation.⁷² However, it seems fairly clear that the court would have hesitated to recognize a claim for injunctive relief. Any truthful public information about the plaintiff would remain public. The court did seem to indicate that the plaintiff should be permitted to escape her former public identity, but it suggests that the defendant would have been wholly permitted to tell her story if it had not used her true name.⁷³ One principle from *Melvin* that has been recognized elsewhere is the possibility that publicizing a person’s past crimes infringes on that person’s ability to rehabilitate and, thus, is a violation of the right to privacy.⁷⁴ In *Briscoe v. Reader’s Digest*,⁷⁵ the court held that references to prior crimes in a widespread publication might infringe on a person’s ability

69. *Id.* at 92 (quoting *Jones v. Herald Post Co.*, 18 S.W.2d 971, 973 (Ky. 1929)).

70. *Id.*

71. *Id.* at 93.

72. *Id.* at 93–94.

73. *See id.* at 93 (“We believe that the publication by respondents of the unsavory incidents in the past life of appellant after she had reformed, coupled with her true name, was not justified by any standard of morals or ethics known to us . . .”).

74. *Cf. Briscoe v. Reader’s Digest Ass’n*, 483 P.2d 34, 40 (Cal. 1971) (recognizing the rehabilitative policy interests as set out in *Melvin*), *overruled by* *Gates v. Discovery Commc’ns, Inc.*, 101 P.3d 552 (Cal. 2004).

75. *Briscoe v. Reader’s Digest Ass’n*, 483 P.2d 34 (Cal. 1971), *overruled by* *Gates v. Discovery Commc’ns, Inc.*, 101 P.3d 552 (Cal. 2004).

to obtain rehabilitation.⁷⁶ The California Supreme Court did not adopt the right to be forgotten in *Melvin* or *Briscoe*, but the court suggested that public figures should have some sort of right to fade away from the public eye.⁷⁷ At first glance, the court seemed to grasp at establishing a right for criminals (or former criminals) to be forgotten. It seems paradoxical to give criminals a right to be forgotten but to decline extending such a right to non-criminals. But as more recent U.S. case law shows, the *Melvin* and *Briscoe* cases are as close as U.S. courts have come to adopting the right to be forgotten, and courts generally decline to extend privacy rights to the outer limits of *Melvin* and *Briscoe*.⁷⁸

2. *Sidis v. F-R Publishing Corp.*⁷⁹

The United States Court of Appeals for the Second Circuit issued the *Sidis* opinion almost a decade after *Melvin*, and the court strongly rejected the *Melvin* court's suggestion that public figure status should fade with time.⁸⁰ The plaintiff in *Sidis* had been a "famous child prodigy" three decades before his lawsuit.⁸¹ After graduating from Harvard University at sixteen years of age, he seemingly disappeared from the public eye.⁸² Twenty-seven years later, when a New York-based magazine featured Sidis in its column "Where Are They Now?" and contrasted his early accomplishments with his ordinary adulthood, Sidis filed suit for invasion of privacy.⁸³ Rather than continue down the path laid out by *Melvin*, the court held against the former child prodigy and refused to recognize a violation of his right to privacy.⁸⁴ In part, the court based its holding on the need to protect freedom of expression, especially when media is involved:

76. *Id.* at 43.

77. *See id.* at 40 ("Where a man has reverted to that 'lawful and unexciting life' led by others, the Restatement implies that he no longer need 'satisfy the curiosity of the public.'").

78. *See Jones v. New Haven Register, Inc.*, 763 A.2d 1097, 1101 (Conn. Super. Ct. 2000) (explaining that when someone becomes a public figure, regardless of whether it is by choice, he remains a public figure, and is of legitimate public interest for life (quoting Prosser, *supra* note 62, at 418)).

79. *Sidis v. F-R Publ'g Corp.*, 113 F.2d 806 (2d Cir. 1940).

80. *Id.* at 807–09; *see Jones*, 763 A.2d at 1101 ("*Melvin* represents something of a high-water mark for the privacy rights of the formerly famous. Nine years later, the Second Circuit reached a quite different conclusion in *Sidis* The analysis of *Sidis* has proven to be much more persuasive than that of *Melvin* in modern times.").

81. *Sidis*, 113 F.2d at 807.

82. *Id.*

83. *Id.*

84. *Id.* at 809.

Regrettably or not, the misfortunes and frailties of neighbors and “public figures” are subjects of considerable interest and discussion to the rest of the population. And when such are the mores of the community, it would be unwise for a court to bar their expression in the newspapers, books, and magazines of the day.⁸⁵

The holding in *Sidis* represents a majority rule that is followed with few exceptions throughout American courtrooms—once public, always public.⁸⁶ This rule is especially true when a person is a public figure with respect to a specific controversy or event and is later involved in public disclosures regarding that controversy or event.⁸⁷

B. *The Restatement (Second) of Torts* § 652⁸⁸

Section 652 of the Restatement Second of Torts recognizes four distinct actions that constitute invasion of privacy, each listed in section 652A and then explained in subsequent separate sections 652B–652E:

- (a) unreasonable intrusion upon the seclusion of another (§ 652B); or
- (b) appropriation of the other's name or likeness (§ 652C); or
- (c) unreasonable publicity given to the other's private life (§ 652D); or
- (d) publicity that unreasonably places the other in a false light before the public (§ 652E).⁸⁹

Subsection (c)—the “publicity given to private life” tort—seems

85. *Id.*

86. See David Libardoni, Note, *Prisoners of Fame: How an Expanded Use of Intrusion Upon Psychological Seclusion Can Protect the Privacy of Former Public Figures*, 54 B.C.L. REV. 1455, 1458–59 (2013) (stating that under the current laws in the United States, there is no way for a former public figure to regain the privacy rights of private citizens and citing several United States cases as examples).

87. See *Partington v. Bugliosi*, 56 F.3d 1147, 1152 n.8 (9th Cir. 1995) (“[T]he passage of time does not alter an individual's status as a limited purpose public figure.”); *Contemporary Mission, Inc. v. N.Y. Times Co.*, 842 F.2d 612, 619–20 (2d Cir. 1988) (discussing how the passage of time does not mean an individual's status will revert from public back to private), *cert. denied sub nom.*, *O'Reilly v. N.Y. Times Co.*, 488 U.S. 856 (1988); *Street v. Nat'l Broad. Co.*, 645 F.2d 1227, 1235–36 (6th Cir. 1981) (concluding a person may retain public figure status regarding a specific event), *cert. granted*, 454 U.S. 815 (1981), *cert. dismissed*, 454 U.S. 1095 (1981); *Brewer v. Memphis Publ'g Co.*, 626 F.2d 1238, 1256–57 (5th Cir. 1980) (considering whether a public figure removed from the public sphere for many years could bring an action for defamation under the *New York Times* standard), *cert. denied*, 452 U.S. 962 (1981); *Wolston v. Reader's Digest Ass'n*, 578 F.2d 427, 431 (D.C. Cir. 1978) (“The mere lapse of time is not decisive.”), *rev'd on other grounds*, 443 U.S. 157 (1979); *Time, Inc. v. Johnston*, 448 F.2d 378, 381–82 (4th Cir. 1971) (comparing the similarities between defamation and invasion of privacy cases and the passage of time element used to distinguish between public and private figures).

88. RESTATEMENT (SECOND) OF TORTS § 652 (AM. LAW INST. 1977).

89. *Id.* § 652A.

congruent to the right to be forgotten.⁹⁰ Both recognize individuals' right to keep to themselves. One apparent difference is that American plaintiffs alleging a claim based on subsection (c) are seeking monetary damages, while a claimant in a right-to-be-forgotten jurisdiction, in addition to or instead of seeking monetary damages, could seek removal of published personal information.⁹¹ Another substantial difference is the seemingly low amount of privacy protection afforded by this invasion of privacy cause of action. Section 652D further explains subsection (c):

One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that

- (a) would be highly offensive to a reasonable person, and
- (b) is not of legitimate concern to the public.⁹²

The act of "giving publicity" in section 652D means making information public.⁹³ To do so, the tortfeasor must go beyond sharing the information with a small group of persons; the public must be likely to receive the information.⁹⁴ In the Internet context, anytime a person posts or uploads information, they are giving that information publicity. However, the additional requirements of subsections (a)–(b)—the "highly offensive" requirement and the requirement that the matter be not of legitimate public concern—severely erode privacy protections for Americans.⁹⁵ Unless the disclosed information would be (1) extremely offensive to an objectively reasonable person, *and* (2) of virtually no public interest, then the subject person would have no tort action for publicity of his private life.⁹⁶

C. *Instances of Internet Censorship Affecting United States Users*

1. Google, Revenge Pornography, and De-linking Web Domains

Several lawsuits and significant media attention surrounding revenge pornography have facilitated a change to Google's traditional philosophy that web searches should reflect the web in its entirety.⁹⁷ The revenge

90. *Id.* § 652C.

91. *Cf. id.* § 652D note (discussing the relationship of public and private life to the First Amendment).

92. *Id.* § 652D.

93. *Id.* § 652D cmt. a.

94. *Id.*

95. *Id.* § 652D cmt. on clause (a), cmt. on clause (b).

96. *Id.*

97. Amit Singhal, "Revenge Porn" and Search, GOOGLE PUB. POL'Y BLOG (June 19, 2015),

pornography epidemic included mostly vindictive postings on the Internet of nude pictures by an “ex” without the other’s consent.⁹⁸ In response, Google amended its policies:

Our philosophy has always been that Search should reflect the whole web. But revenge porn images are intensely personal and emotionally damaging, and serve only to degrade the victims—predominantly women. So going forward, we’ll honor requests from people to remove nude or sexually explicit images shared without their consent from Google Search results. This is a narrow and limited policy, similar to how we treat removal requests for other highly sensitive personal information, such as bank account numbers and signatures, which may surface in our search results.⁹⁹

Google made this calculated decision by weighing the utility of public access to revenge pornography with the damage suffered by individual victims of revenge pornography. This change is somewhat indicative of Google’s ability to recognize the intersection of the right to privacy and freedom of speech and respond correctly. Several other search engines have amended their policies to adopt similar exceptions.¹⁰⁰ However, this policy implementation only included Google searches and Google images. In most instances, the original pictures on their respective revenge pornography websites remained. This fact highlights a significant problem with the practicality of the right to be forgotten. It is wholly impractical to remove content from the Internet effectively because of the ease in which content is duplicated and transferred among users. De-linking specific websites or images does little to prevent content from reappearing, and content usually remains in its original location where people can continue to find it by typing in specific URLs into their browsers. Those specific URLs that have been de-linked from search engines are often circulated on message boards such as Reddit and 4chan. A tactic which might produce better results, but would have an impermissibly chilling effect on the freedom of expression, would be to de-link Reddit and 4chan-type websites from search engines—something Google has actually done before.¹⁰¹

<https://googlepublicpolicy.blogspot.com/2015/06/revenge-porn-and-search.html>.

98. *Id.*

99. *Id.*

100. *Google Privacy Policy Changes Spark Europe-Wide Inquiry*, GUARDIAN (Feb. 29, 2012, 11:16 PM), <https://www.theguardian.com/technology/2012/mar/01/google-privacy-policy-changes-eu>.

101. Sam Machkovech, *8chan-hosted Content Disappears from Google Searches*, ARS TECHNICA.COM (Aug. 17, 2015 11:43 AM), <https://arstechnica.com/tech-policy/2015/08/8chan-hosted-content-disappears-from-google-searches>.

2. Erasure Button Laws

Effective as of January 1, 2015, California's Children's Online Privacy Protection Act ("CalOPPA")¹⁰² is the first law of its kind aimed at protecting minors online.¹⁰³ One way the law does this is by prohibiting companies from marketing products to minors that are otherwise prohibited to be sold or marketed to children offline, such as tobacco and alcohol.¹⁰⁴ However, the aspect of the law that has caught the public's attention is the so-called "eraser button," which requires Internet companies to provide a method by which minors can delete a posted picture from a website.¹⁰⁵ Websites must provide clear instructions to minors as to how they may remove content they have posted online, and the website may be required to make certain content invisible to other website users.¹⁰⁶ Supporters of CalOPPA and similar legislation argue that such "eraser buttons" can protect teenagers, which as a demographic are avid users of social media¹⁰⁷ and whose youthful online posts could come back to haunt them days, weeks, or even years after they are published online.¹⁰⁸ These proponents tie the need to be able to remove Internet content posted by an individual to that individual's maturity, recognizing that teenagers often "self-reveal before they self-reflect."¹⁰⁹ Enabling teenagers to remove any content they

102. S.B. 568, 2013 Leg., 2013–14 Sess. (Cal. 2013).

103. See Andrea Peterson, *Author of California Online Eraser Law: It's Not Always Easy to Find the Delete Button*, WASH. POST (Sept. 25, 2013), <https://www.washingtonpost.com/news/the-switch/wp/2013/09/25/author-of-california-online-eraser-law-its-not-always-easy-to-find-the-delete-button/> (explaining the "eraser" provision of the new law which allows minors to delete content posted by themselves).

104. See *id.* (observing one aspect of the law is to ensure marketing restrictions that exist outside the Internet are enforced online as well).

105. Deborah Hastings, *Unprecedented 'Eraser Button' Law in California Gives Teens New Internet Life*, N.Y. DAILY NEWS (Sept. 24, 2013, 5:33 PM), <http://www.nydailynews.com/news/national/calif-measure-kind-teenagers-erase-internet-article-1.1466400> (describing the law as a tool for minors to "erase online writings that could become digital skeletons").

106. See CAL. BUS. & PROF. CODE § 22581 (Deering Supp. 2016) (requiring websites to post clear instructions to minors on how to remove content posted on the website).

107. See Mary Madden et al., *Teens, Social Media, and Privacy*, PEW RES. CTR. 19 (2013), <http://www.lateledipenelope.it/public/52dff2e35b812.pdf> (reporting that eight in ten teen Internet users also use some kind of social media).

108. See Caitlin Dewey, *How the 'Right to Be Forgotten' Could Take Over the American Internet, Too*, WASH. POST (Aug. 4, 2015), <https://www.washingtonpost.com/news/the-intersect/wp/2015/08/04/how-the-right-to-be-forgotten-could-take-over-the-american-internet-too/> (explaining how one high school student's racist tweet became national news and how teens' social media posts often fall into the hands of college admissions officers and employers years after the content was put on social media).

109. See Dewey, *supra* note 108 (relaying position of Jim Steyer, founder and chief executive of Common Sense Media, regarding privacy for teenagers' social media posts); see also Somini Sengupta, *Sharing with a Safety Net*, N.Y. TIMES (Sept. 19, 2013), <http://www.nytimes.com/>

regret, or simply do not care to share anymore, means those impulsive over-sharing or inappropriate posts will stay in the teenage poster's past—preventing a digital lapse in judgment from haunting them through every job interview of their adult life.¹¹⁰ Critics of the law see the ability of an individual to effectively redact their online history as a slippery slope—how much should an adult be able to retract from Internet posts made as a teenager? CalOPPA allows for the erasure of content posted by the individual but not content posted by someone else.¹¹¹ But should a person also be able to delete content about them that someone has re-shared—or content about them that was originally posted by someone else?

Other critiques of the law include practicality issues, asserting, for instance, that “companies [will] be forced to devise multiple policies for the underage residents of different states” if other states pass laws similar to CalOPPA.¹¹² Another argument in opposition to eraser button laws asserts that the laws, in an attempt to protect minors online, might force website users to divulge more information to Internet companies, such as their age and state of residence.¹¹³ Moreover, CalOPPA may face issues with the Dormant Commerce Clause because it is neither limited to websites based in California nor used only by people in California. This problem extends to websites based in other states but available for users in California.¹¹⁴ Other critics think the law does not go far enough. CalOPPA requires that minors be able to remove content they have posted on the Internet or request that it be de-linked. However, if that content has already been shared, it will remain in the “shared” location on the Internet. While the de-linked websites will not appear in search engine results, the content remains

2013/09/20/technology/bill-provides-reset-button-for-youngsters-online-posts.html (quoting Steyer as arguing that minors do not fully comprehend the effects and consequences of their online posts).

110. See Dewey, *supra* note 108 (explaining “nearly half of all hiring managers, and a third of all college admissions officers” consider an applicant’s online presence).

111. See *id.* (discussing the limitation of deletion privileges under CalOPPA, which extend only to personally posted content, and pointing to the danger of allowing individuals to delete content posted by someone else); see also Eric Goldman, *California's New 'Online Eraser' Law Should Be Erased*, FORBES (Sept. 24, 2013, 1:35 PM), <http://www.forbes.com/sites/ericgoldman/2013/09/24/california-new-online-eraser-law-should-be-erased/#7e8c99f4399d> (outlining several problems relating to CalOPPA).

112. Sengupta, *supra* note 109.

113. *Id.*

114. See James Lee, Note, *SB 568: Does California's Online Eraser Button Protect the Privacy of Minors?*, 48 U.C. DAVIS L. REV. 1173, 1177 (2014) (arguing state-by-state regulation of online privacy is unconstitutional under the Dormant Commerce Clause, which prohibits states from enacting laws that discriminate against or overly burden interstate commerce and arguing in favor of federal laws similar to Europe’s right to be forgotten).

on the search engine servers and on the website hosting the content.¹¹⁵

IV. CONCLUSION

While Europe's right to be forgotten has opened the floodgates to waves of requests to search engines for the deletion and de-linking of information, no such right exists for similar requests in the United States. Proponents of such a right for U.S. citizens call for laws to protect personal privacy as more and more data is collected about individuals and hosted online, available to anyone with the stroke of a Google search.¹¹⁶ Supporters of the right to be forgotten in the United States argue that this protection is needed to reassert a realm of privacy that has drastically shrunk or even disappeared with the rise of the Internet.¹¹⁷ But while the idea of an eraser button seems like an attractive option for those blurry-eyed and solo-cup-filled photos and teenage angst-ridden tweets that we would like to prevent from showing up in a college admission officer's or job recruiter's due diligence, the right to be forgotten encompasses more than the ability to delete embarrassing college Facebook posts. The practical application of such a right amounts to censorship and runs counter to well-established U.S. First Amendment rights.¹¹⁸ Moreover, as the debate continues as to whether such a right should exist in U.S. law, lawmakers may find that public opinion disfavors a right to be forgotten.¹¹⁹ Instituting the right to be forgotten risks the suppression of collective memory.¹²⁰ Although content that is de-linked from search engine results remains on the actual website on which it is published, such information is all but useless if it is not accessible through a search engine.¹²¹ Arguing that de-linking is not censorship because the

115. See Sengupta, *supra* note 109 (noting CalOPPA does not require Internet companies to completely remove deleted data from their servers or provide a means to delete material that has been shared by others—"a sensational picture that has gone viral, in other words, can't be purged from the Internet").

116. See Roberts, *supra* note 39 (quoting European Commission official Paul Nemitz, who favors the U.S. following Europe's model of the right to be forgotten).

117. See *id.* (discussing a debate hosted at the Kaufman Center in New York City between Nemitz and Professor Eric Posner, supporters of the right to be forgotten, and Digg CEO Andrew McLaughlin and Professor Johnathan Zittrain, opposing the adoption of such a right in the United States).

118. See generally Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 458 (1980) ("The limits of law in protecting privacy stem . . . from the law's commitment to interests that sometimes require losses of privacy, such as freedom of expression, interests in research, and the needs of law enforcement.").

119. See Roberts, *supra* note 39 ("At the end of the [Kaufman Center] debate, the attendees voted 56% against the notion that the U.S. should adopt a right to be forgotten law.").

120. See *id.* ("The right to purge Google, in this sense, is no more than a new form of censorship that provides encouragement to dictators everywhere.").

121. See Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)*,

data is deleted from the search engine but not from the entire Internet is tantamount to allowing a book to remain on library shelves but redacting all of the pages. Admittedly, exponentially more personal data is collected and published on the Internet today than anyone could have imagined even fifty years ago, and protections are needed to prevent private companies from invading individuals' reasonable expectations of privacy.¹²² However, our culture is already taking note of the consequences of living life online, and the same teens that eraser button laws are being designed to protect are moving their digital lives to digital platforms that purportedly carry less risk of creating a permanent Internet embarrassment.¹²³ Between 2013 and 2015, the percentage of college admissions officers who reported that social media had negatively affected a student's admission chances fell from 35% to 16%.¹²⁴ Perhaps adults should take a cue from the kids on this one by taking advantage of the privacy controls offered by social networks and recognizing that what you post online creates a digital, searchable trail.¹²⁵ Internet companies continue to evolve their privacy protocols in response to public sentiment surrounding issues such as cookie tracking and location based services.¹²⁶ Meanwhile, our culture continues to accept the occasional embarrassment of a regrettable social media post from a time when we did not fully grasp the longevity of these platforms and webpages. An entire industry is emerging as the private sector sees an opportunity to help individuals clean up their digital presence and maintain a respectable online image.¹²⁷ The best approach for the United States is to avoid constitutionality issues with the so-called "right to be forgotten" by

2014 E.C.R. I-317, <http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN> (discussing the limits of accessibility of information on the Internet without the use of search engine results).

122. See Roberts, *supra* note 39 (reporting Nemitz's comments from the Kaufman Center debate on how companies like Google and Facebook erode personal privacy by collecting and selling personal information of their users).

123. See Dewey, *supra* note 108 ("Everyone knows that if you want to say something racist in this day and age, you better say it on an anonymous app [such as Whisper and Snapchat].").

124. See *id.* (relaying the percentage of admissions officers who said a prospective student's chances of admissions have been hurt by social media has fallen in recent years).

125. See *id.* (quoting a teen who calls Facebook "parentland" and says teens are beginning to self-censor their own profiles on the platforms that create more permanent digital trails).

126. See Jeffrey Rosen, *The Web Means the End of Forgetting*, N.Y. TIMES (July 25, 2010), <http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?pagewanted=all> (reporting changes to Google policies to "render all search queries anonymous after nine months" and an announcement by search engine Cuil that the company will not "keep any personally identifiable information" of its users, and discussing a technology called Vanish that uses encryption technology to destroy electronic data after a certain period of time).

127. See *id.* (discussing companies like ReputationDefender, which monitors the online reputations of customers in more than 100 countries).

2016]

THE RIGHT TO BE FORGOTTEN

275

declining to adopt such a right, and instead allowing public feedback to the private sector to continue to advance online privacy expectations.